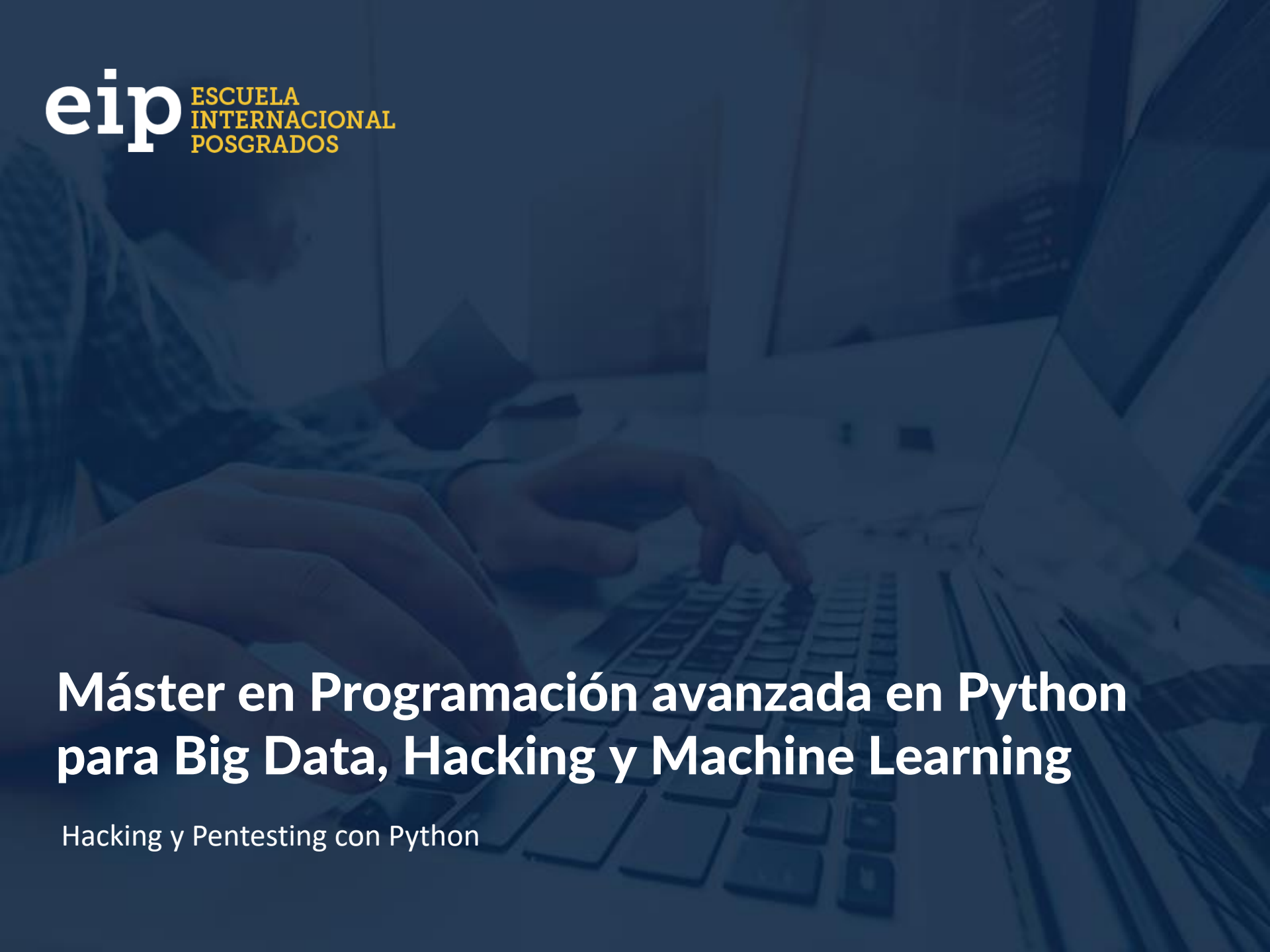

ESCUELA INTERNACIONAL POSGRADOS

Máster en Programación avanzada en Python para Big Data, Hacking y Machine Learning

Hacking y Pentesting con Python

MÓDULO 02

Fingerprinting y Banner grabbing.

Banner Grabbing

Se trata de una técnica utilizada en la etapa de enumeración que permite enumerar los servicios que pueden tener vulnerabilidades conocidas en el sistema objetivo.

Para ejecutar este tipo de procedimientos, normalmente se debe contar con un listado de "banners" que contienen patrones de servicios vulnerables conocidos.

Dado que en los banners se suele incluir información sobre la versión y tipo de servicio que se está consultando, esta técnica es útil para determinar las características básicas del servicio remoto.

Herramientas como Nmap aplican técnicas de "banner grabbing" para detectar las versiones de cada servicio en ejecución.

Integración entre Metasploit Framework y Python

Metasploit cuenta con una interfaz de acceso remoto llamada MSGRPCD.

La interfaz MSGRPC utiliza el formato MessagePack para el intercambio de información entre la instancia de Metasploit Framework y los clientes.

Para crear un cliente en Python que pueda interactuar con el servicio MSFRPCD, se utiliza la librería “pymetasploit3” que tiene todo lo necesario para interactuar con la API de Metasploit Framework.

La librería “pymetasploit3” depende de la librería “msgpack” para manipular los mensajes con formato MessagePack.

Es recomendable conocer la API de Metasploit Framework (Metasploit Remote API): https://community.rapid7.com/docs/DOC-1516

MUCHAS GRACIAS POR SU ATENCIÓN

eip ESCUELA INTERNACIONAL POSGRADOS


decheverri@grupomainjobs.com


Daniel Echeverri
https://www.linkedin.com/in/adastra1/


twitter.com/eiposgrados


facebook.com/eiposgrados


instagram.com/eiposgrados